	DEPARTMENT OF CORRECTIONS **Institutions**	
Title:	**Operations Division Security Audits**	**DOC Policy: 40.1.4**
Effective:	**03/08/18**	**Supersedes: 11/01/16**
Applicability:	**Institutions and Non-Institution Facilities**	
Directives Cross-Reference: None		
Attachments: Form – Request for Variance / Exception (CD1737)		

I. PURPOSE

To provide guidelines related to the Operations Division Security Audits used to measure facility security and operational standards on a department-wide level.

II. DEFINITIONS

A. Corrective Action Plan: A written process to be used by the functional unit manager or designee to show planned action to be taken, and time frames to correct all "not compliant" findings of the Operations Division Security Audit.

B. Internal Security Audit: A process established by the functional unit manager by which each facility continuously monitors throughout the audit year the facility's compliance with DOC Policies, and the state of facility readiness for any scheduled or unannounced audit or actual incident that may occur.

1. The facility internal audit may be conducted as a formal audit, for which the functional unit manager or designee assigns an employee or group of employees to physically and formally audit and document the facility's performance.

2. The facility internal audit may be conducted through a check and balance system such as the facility's performance score card and measurables.

C. Operations Division Audit Instrument: A printed document that acts as an aid to security auditors during the course of an audit to define standards, relate issues to specific policy statements, and record observations/notes of the auditor.

D. Policy and Audit Standard Exception: A written process (Request for Variance / Exception CD1737) used by the functional unit manager or designee to express the need and to request to operate in a manner that contradicts department policy

E. Security Auditor: A DOC security management employee assigned by the Emergency Manager and Chief of Security, who has received classroom and on-the-job training, and is responsible for maintaining the integrity of the audit system while conducting facility audits.

F. Security Audit Team Leader: A DOC security management employee who is part of the Security Audit Team and assigned by the Emergency Manager and Chief of Security. The Security Audit Team Leader is trained and experienced in conducting facility security audits, is responsible for maintaining the integrity of the audit system while conducting facility audits, is responsible for the final report, and assisting with the on-the-job training of new auditors.

G. Security and Operational Standard: A type or degree of requirement in operations which implies the highest form of excellence in security and operational practices. Standards are found in policy or mutually acceptable practices in the profession.

H. Variance: A written process (Request for Variance / Exception CD1737) used by the functional unit manager or designee to request extra time and to show the intent of requesting assistance/resources outside of the facility to achieve compliance with written policy/standard. Variance approvals are only valid for one year.

III. POLICY

The Department of Corrections shall provide a high level of safety and control through quality security and operational standards and methods to measure compliance.

A. Audit Philosophy and Goals

1. Provide an unbiased, non-threatening, valuable management service to each facility administration.

2. Provide each facility a measurement of compliance with departmental policy.

3. Provide a forum of constructive, proactive approach among peers in the search for more effective and efficient methods of operating security and operational programs.

4. Provide professional development for staff.

5. Provide a pathway for the expression of ideas for improvement in department policy.

6. Provide consistency and standardization of security systems, operation application, equipment, policy, and procedures.

B. Provision of Auditors and Audit Coordinators

1. Auditors may be any DOC security management employee who has demonstrated experience and knowledge of DOC rules and policies, institutional safety and security operations, and the ability to work in a collaborative and respectful manner.

2. Audit team leaders will be any DOC security management employee with experience and training as a security auditor. Audit team leaders will be

designated by the Emergency Manager and Chief of Security and identified on the audit schedule.

3. Auditors will remain on the audit team and will be available for a period of time as recommended by the Chief of Security, and approved by the Assistant Director for Operations. No more than half the team will rotate off at a time to ensure continuity from past to present team members.

    a. To maintain the integrity, consistency, and accuracy of the audit system, and provide adequate auditor training, there may be two teams of auditors to lessen the burden to the facilities providing security managers for the teams.

    b. Each audit team should be made up of four auditors. Two auditors as identified and assigned by the Chief of Security will perform the duties of lead auditor and trainers, auditing all facilities. The remaining four auditors will each audit approximately half of the facilities.

4. Each year new auditors may be selected with the exception that one of the lead auditors will remain on the team to continue as a lead auditor and trainer. If the second lead auditor is replaced, the replacement lead auditor and trainer will be selected from one of the auditors trained and experienced from the previous year.

5. A confidential schedule of security audits shall be created by the Emergency Manager and Audit Team Leader.

6. Operations Division Security Audits shall be performed at least annually. The schedule shall include the dates and locations of the audits, list the names of the Audit Team Leader and the auditors for the team.

C. Operations Security Audit Process

1. In January of each year, every facility will send the Chief of Security or designee, facility specific post orders, procedures, and/or any other written directives that show compliance in the department polices requiring written directive in the specific areas being audited.

    a. The Chief of Security or designee will provide the Security Audit Team Leader a copy of each facility's written directives pertaining to the audit standards, the facility's previous audit results, the After Action Report, any variances or exceptions granted, DOC policies/procedures related to the Operations Security Audit, and the Operations Division Audit Instrument.

    b. The Audit Team Leader and audit team will review the facility documentation, reporting compliance or non-compliance of these areas prior to the facility audits. The facilities may correct any non-compliance pertaining to written directive areas up to and until the beginning of the start of the physical audit.

2. The Operations Security Audit is unannounced; therefore, the first day of the facility audit will begin no earlier than 8:00 am on a weekday. Upon arrival to the

facility, the audit team will announce their presence and meet with the functional unit manager or highest ranking onsite employee.

3. Facilities will provide the audit team with any updated written directives and other requested documentation. These and other documents will be reviewed during the audit process.

4. A room will be made available to the team at the audit site. Staff will be made available to facilitate access to any and all areas of the facility and to answer specific operational questions. The audit preparation is designed to be supportive, provide quality audit results, and to follow up on the previous audit's after action plans.

5. An exit interview will be scheduled with the audit team and facility members, as determined by the functional unit manager or designee.

D. Facility Internal Audits

1. Each facility will conduct quarterly internal audits of the same area/standards or policies reviewed by the Security Audit Team. The facility may choose to skip the quarterly internal audit that falls within or directly after the facility's Security Audit.

   a. Armory
   b. Inmate Counts
   c. Key Control
   d. Perimeter Security
   e. Tool Control

2. Each facility will conduct annual internal audits of the following areas/standards, and any area determined by the Chief of Security:

   a. Admission and Discharge
   b. Communications
   c. Contraband & Evidence Mgmt
   d. Control Centers
   e. Controlled Movement
   f. Emergency Preparedness
   g. Food Service
   h. Hazardous Material Mgmt
   i. Information Security
   j. Inmate Mail
   k. Inmate Visiting
   l. Inmate Property
   m. Inmate Work Assignments
   n. Inmate Transportation
   o. Medical Services
   p. Physical Plant
   q. Post Orders
   r. Safety and Fire Safety
   s. Searches
   t. Security Inspections
   u. Special Housing
   v. Use of Force

E. Operations Security Audit Reporting

1. All conclusions of auditors shall be indicated in the audit report. The audit report shall be compiled from the audit instrument and observations of the audit team, which are verbally communicated to administration during the exit interview at that conclusion of the site visit. The audit report will be due to the Chief of Security, and functional unit manager within 30 calendar days of the site visit.

2. Within 30 calendar days of the receipt of the audit report, the facility shall address discrepancies, make recommendations, and complete an after-action response. The after-action response will be submitted the Chief of Security.

a. The facility functional unit manager or designee may submit a variance request on form CD1737.

b. On the rare occasion the facility functional unit manager or designee finds it in the best interest of the department and the facility to make a request to operate in a manner that contradicts department policy, the functional unit manager or designee will submit a request for a policy exception on form CD1737.

c. Prepare a Variance/Exception form CD1737 for the Institutions Administrator and the Chief of Security to be emailed to the Operations' Administrative Specialist at Central Office and include the following:

    1) Cite the Audit Standard and number that was found in Non-Compliance and include any Auditor's remarks.

    2) Detail the issues and/or conflicts that are causing your institution to be in non-compliance.

    3) Describe in detail what intermediary actions will be put in place to ensure the deficiency will not continue to compromise security.

    4) Describe in detail of what actions you are taking to overcome the issue of non-compliance and alleviate the need for the variance.

    5) If seeking a variance, cite the forecasted time needed to become compliant in the standard.

    6) If seeking an exception, describe in detail why the facility cannot meet the established standard.

d. Operations' Administrative Specialist will forward the Variance/Exception request to the appropriate Emergency Manager and Lead Auditor for review. The Emergency Manager and Lead Auditor will conduct the following:

    1) Review the request for completeness and ask for any additional information necessary.

    2) Emergency Manager and Lead Auditor will discuss the request to ensure the submitting institution's request is in line with the intent of the standard.

    3) Develop a recommendation to the Chief of Security for issuance, denial or reinstatement of the request.

e. The Chief of Security will review the circumstances to determine if an exception to policy is appropriate to forward to the Assistant Director for Operations for approval.

    1) If the facility's request is approved, the Chief of Security will consider the necessity and appropriateness for a department policy change.

2) If the facility's request is approved and the policy will not be changed, the facility's functional unit manager will address the exception and approval in writing within the facility procedure.

3) Variances are only good for one year from the approval date.

F. Facility Internal Audit Reporting

1. Each facility will forward a copy of the results of their internal audit, a copy of the after action response for any areas not meeting policy standards, and any request for variances or exceptions to the Chief of Security within 30 calendar days of completion of the internal audit.

2. Each facility will utilize their score card to track the results of the facility's audits (facility internal audits and Security Audit Team findings).

G. Training

1. Operations Division Security Audits team members will receive documented, formal classroom training before beginning any audits.

2. Team members will receive documented, in depth on-the-job auditor training.

3. Classroom training may be accomplished in person, or via an on-line learning experience. Classroom training shall address the DOC security audit philosophy, goals, and role of the auditors, benefits of security auditing, specific DOC policies and areas to be audited, and the overall process.

4. On-the-job training will ensure each team member is thoroughly familiar with all of the relevant policies and how to apply them in each facility.

K. Non-institution Facilities

1. The Transport Unit will be audited on the Armory and Keys and Locks policies.

2. All other non-institution facilities will be audited on the Keys and Locks and Tool Control policies as determined by the Chief of Security.

V. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: ____signature on file _____
Michelle Mooney, Rules Coordinator

Approved: ___signature on file_____
Brian Belleque, Deputy Director